

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
3 July 2003 (03.07.2003)

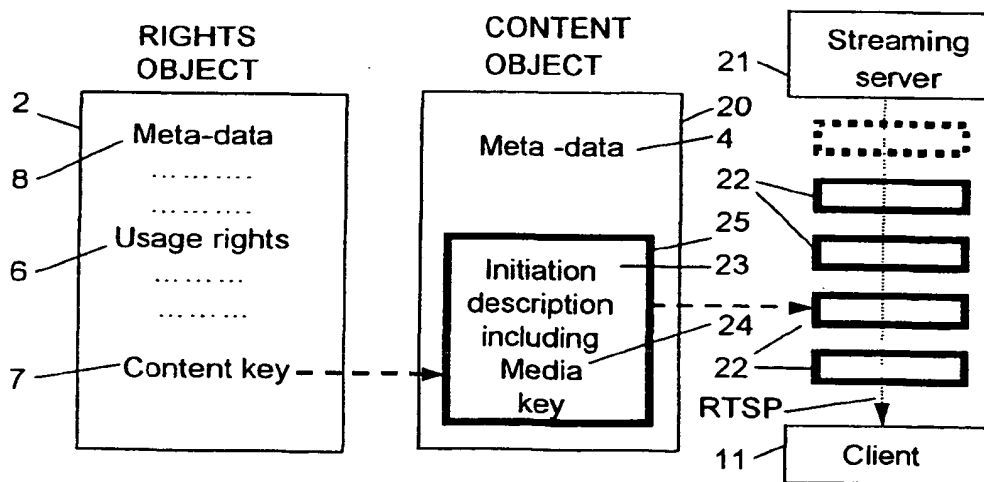
PCT

(10) International Publication Number
WO 03/055219 A2

- (51) International Patent Classification⁷: **H04N 7/24** (74) Agent: **DR LUDWIG BRANN PATENTBYRÅ AB**; Box 1344, Drottninggatan 7, S-751 43 Uppsala (SE).
- (21) International Application Number: **PCT/SE02/02292**
- (22) International Filing Date:
10 December 2002 (10.12.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
60/338,686 11 December 2001 (11.12.2001) US
- (71) Applicant: **TELEFONAKTIEBOLAGET LM ERICSSON (PUBL.)** [SE/SE]; S-126 25 Stockholm (SE).
- (72) Inventors: **SELANDER, Göran**; Bergsundsgatan 25, S-117 37 Stockholm (SE). **LINDHOLM, Fredrik**; Stångatan 87, S-125 74 Älvsjö (SE). **BLOM, Rolf**; Svärdvägen 2, S-175 68 Järfälla (SE).
- (81) Designated States (*national*): AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, OM, PH, PL, PT, RO, RU, SD, SE, SG, SK (utility model), SK, SI, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD OF RIGHTS MANAGEMENT FOR STREAMING MEDIA



(57) Abstract: The present invention relates to an arrangement, system and method for managing rights to streaming media using a management mechanism based on a content object and a rights object. In accordance with the invention the content object comprises means for initiation of the streaming media and the rights object comprises usage rules defining the rights to use said streaming media. The invention also relates to a method of delivering and protecting digital streaming media. The initiation may comprise a session description of the streaming media, a SDP description, a URL to said streaming media or a SMIL file. Preview and super-distribution are provided. The content object is delivered like a downloadable object in a rights management system for download, thereby reusing the mechanisms for rights management of said latter system for rights management in a system for transmission of streaming media.

WO 03/055219 A2

WO 03/055219 A2



Published:

— without international search report and to be republished
upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

METHOD OF RIGHTS MANAGEMENT FOR STREAMING MEDIA

TECHNICAL FIELD

The present invention generally relates to rights management (Digital Rights Management)
5 for managing digital content provided over networks, and more particular to methods, equipment and systems used for managing rights for streaming media.

BACKGROUND

The distribution of digital content or media data using modern digital communication technologies is constantly growing, increasingly replacing the more traditional distribution
10 methods. In particular, there is an increasing trend of downloading or streaming digital content over a network from a content provider to a client or user, which then typically renders the content using a rendering device according to some user rights, or usage rules specified in a license associated with the digital content. Due to the advantages of this form of content distribution, including being inexpensive, fast and easy to perform, applications can now be
15 found for distribution of all types of content such as audio, video, images, electronic books and software, in particular mobile telephony specific content such as ring signals and background images for the screen of the mobile telephone.

However, with this new way of distributing digital media content comes the need for protecting the content provider's digital assets against unauthorized usage and illegal copying.
20 Copyright holders and creators of digital content naturally have a strong economic interest of protecting their rights, and this has lead to an increasing demand for rights management (DRM). DRM is generally a technology for protecting the content provider's assets in a digital content distribution system, including protecting, monitoring and restricting the usage of the digital content as well as handling payment. A DRM system thus normally includes
25 components for encryption, authentication, key management, usage rule management and charging.

The most basic threats to a DRM system include eavesdropping, illegal copying, modification of usage rules, and removing DRM protection and re-distributing unprotected content for large scale unauthorized usage. Most of these basic security problems are solved by standard

cryptographic techniques, including encryption, authentication, integrity protection and key management. However, what basically distinguishes the security problems of a DRM system from other general security problems is that not even the other end-part of the communication (the user) is completely trusted. In fact, the end-user might want to try to fraudulently extend his usage rights, for example rendering the media content more times than he has paid for or illegally copying the digital content to another rendering device. Therefore, some form of rule-enforcement is required in the client's rendering device. To this end, a DRM agent or module implemented as software and/or tamper-resistant circuit in the rendering device and some formal language expressing the usage rules are commonly used together with the basic cryptographic techniques mentioned above. For a general background in cryptography, we refer to [HAC].

While all the media types mentioned above could be downloaded to a user's device using reliable transport protocols, for real time applications and for other reasons it is sometimes desirable to digitally stream media, such as music or video, to the client. To stream media means to transfer data in a continuous flow to a client in an efficient way that allows for usage of the data before the entire media data has been received. Examples where streaming is more feasible than download include live sports events or music concerts or other media with long duration where it is not feasible, e.g. due to real time or storage requirements, to download the entire or parts of the media before rendering. Streaming is usually carried using unreliable transport mechanisms which might result in errors or losses of data portions. (We do not consider "progressive download" to be streaming, more of this below.) The rationale for using an unreliable transport mechanism is that the real time requirements are so high that there may be no time for resending lost media data, and the risk for quality loss is sometimes acceptable and/or managed by error correction codes or other technical measures. Due to the differences mentioned here, intrinsic and due to differences in transportation, download and streaming of media require different measures for protection of content and in turn require special treatment when managing the rights. The difference is accentuated in a wireless network, such as a mobile telephony network, where disturbances and data loss is more frequent than in a wired network.

The present invention includes in particular a solution which is common to DRM for download content and DRM for streaming media. This solution can be implemented with

virtually no impact in an existing system for download DRM protecting content and managing rights.

STATE OF THE ART

The following is a description of the present techniques of rights management for "content" to be used by a client. Content is generally referred to digital data objects and can be downloaded using a reliable transport protocol (such as TCP, more of which later). Examples of downloadable digital content include audio, video, images, electronic books and software, in particular mobile telephony specific content such as ring signals and background images for the screen of the mobile telephone. To the content is associated a license specifying the client's usage rules and rights pertaining to the obtained digital media.

DRM is about managing the digital content itself and deals with issues such as, who gets it, how is it delivered, how may it be used (rendered, saved, forwarded, copied, executed and/or modified), how many times may it be used, how long does the rights last, who gets paid, how much they get paid and how. Some or all of these issues may be specified in the license, which may be delivered together or separate with the digital content. In order to describe the usage rules, special languages called rights expression languages have been developed. Two of the most prevalent rights expression languages used today are eXtensible Rights Markup Language (XrML), and Open Digital Rights Language (ODRL).

The most difficult part of DRM is to enforce the usage rules included in the license and prescribed for the digital content. As indicated in the background, cryptographic techniques in combination with tamper resistant equipment are common components in existing DRM - solution schemes. Also, obfuscation techniques such as relying on secret algorithms and protocols are used in this context, mainly in proprietary solutions since both security evaluation and interoperability between different solutions are hampered by this means.

The most common data structure for download DRM is based on a separation of the content and the rights to use the content, while maintaining an association between the content and the usage rights. Both content and rights is needed to use the content. One example of DRM download will first be described with reference to Fig. 1 and later some variations, mainly with regards to the protection of content and rights, are given.

In the example of Fig. 1 the part containing downloadable content is referred to as a "content

object” or “content container” 1. The part containing usage rights will be denoted “rights object” 2. Other synonyms of a rights object are “ticket” or “license”. The content object contains the actual digital content 3 and meta-data 4. The content is most often stored in protected form, e.g. encrypted and integrity protected as symbolized by the heavy rectangle 5.

5 The rights object contains usage rights 6, typically expressed in a rights expression language, a content cryptographic key 7, and meta-data 8. With use of the content key the protected digital content can be checked for authenticity and the clear text digital content extracted. The meta data in the content object may contain an identity of the content object, information on the actual content, name and location of the rights holder, information relevant for the
10 rendering of the content such as relevant application or content type, reference to a location where an associated rights object could be accessed/purchased e.g. a Uniform Resource Locator (URL) to a web server hosted by the content provider/distributor. The meta-data of the rights object typically contains a reference to which content object it applies to, such as the content object identity or a (keyed) hash of the encrypted content. Usually, a given rights
15 object is associated uniquely to a particular content object. Sometimes a given content object may have several associated rights objects; one reason for this is to enable different usage of the same content without necessarily changing the content object. One and the same content may be encrypted with different encryption keys and stored in different content objects for security reasons, so that disclosure of a particular secret content key does not reveal the clear
20 text content to all owners of a content object with that particular content, but only to those that have the particular content objects that are encrypted with this key.

A variation on the example above is that the entire content object is integrity protected, not just the content. Another variation is to encrypt the content key in the rights object with an encryption key, and that the so encrypted content key is stored in the rights object instead of
25 the clear text content key. Yet another variation/complement is that the rights object also includes, in addition to what is mentioned above, an “authentication tag”. This tag is included for integrity protection of the usage rights and/or the content key, which can be clear text or encrypted, and/or the meta data. At least the rights are important to integrity protect, since otherwise a fraudulent user could change the granted rights to his favour without consulting
30 the rights owner or paying extra. The security management of the rights object or, if applicable, of the cryptographic key necessary to access the content key, verify the integrity

of the rights etc. is extremely important for the security of the DRM scheme but is not discussed further in this text.

With reference to Figs. 2-4 an example of content download and how a DRM mechanism operates will be described in connection with a user that purchases rights to use some digital content. The example also demonstrates how the DRM mechanism works to enforce that these rights are maintained to ensure that the content cannot be used to others or by other means than what is granted in the rights object. An example of two or more users sharing a media experience is also given.

In the example shown in Fig. 2 a system for DRM of downloadable content comprises a distribution server 9, rights server 10, a client 11 and a DRM broker 12. The distribution server stores and forwards content objects and rights objects. The rights objects are purchased by a user and forwarded to the client. The rights server stores rights objects corresponding to content objects for use when purchasing rights to a previously obtained content object. The client is a device on which the content is rendered. In the client there is a DRM agent 13 to enforce the usage rules. The DRM broker is a network entity that interconnects different right servers, possibly in different networks (not displayed), and offer a single point of contact for a client.

Refer to Fig. 3. A user operating the client browses a web page on the distribution server for content that can be downloaded to the client. The user decides for a particular content with certain rights associated and provides information necessary for making the payment. The user sends a request 14 for the desired content to the distribution server. A content object and a rights object with the appropriate cryptographic protection for this particular client and/or user are delivered to the client, arrows 15 and 16, preferably using a reliable transport mechanism. Within the DRM agent in the client, the necessary cryptographic information is gathered to use the content in the content object in accordance with the usage rights in the rights object. In a practical implementation, trusted applications are necessary to securely render content. The DRM agent parses the rights in the rights object, decrypts content (or request decryption of content from another trusted part, such as a local crypto module in the client) and forwards to the appropriate trusted application to render or use the content according to the specified rights. The application depends on the content type, e.g. the

rendering of music or video is forwarded to a media player application, displaying of images to a picture viewer application etc.

A desired alternative procedure is that the user is allowed to download the content object to the client without or with a special rights object and is by this means able to use a limited version of the full content. This could e.g. be a small portion of a multimedia content such as a 10 second audio clip excerpt of a piece of music, a low resolution version of an image etc. The concept of allowing limited usage for free or to reduced cost is known as "preview", though it may have nothing to do with viewing or displaying the content. The complete rights to the content should not be possible to reveal by this mechanism, e.g. because the content in the content object is cryptographically protected and the content key necessary for using the entire content is located in the (ordinary price) rights object. After preview, the user can decide if the content is desirable to purchase and then contact the rights server, the URL of which may be available from the content object or via the DRM broker, and subsequently purchase and download a rights object needed in the DRM agent to be able to use the entire content.

The separation of content and usage rights utilized in preview is also applied in another desirable content distribution example outlined below: Super-distribution. Refer to Fig. 4. Consider the case that a user wants to share the usage experience with another user. Since the content object is protected in itself and requires no particular security during transport, there is no security risk in sending the content object directly between the two clients, e.g. over a local connection such as Bluetooth, IrDA, cable or by any network.

User B has experienced a interesting content and orders client B to forward the content object to client A which is indicated at arrow 17. The received content object may contain a preview to make it easier for the receiving user to decide if this is interesting. The content object contains a reference to the relevant rights server or DRM broker, which can direct the user to the correct rights server. Client A connects to rights server, negotiates rights, accepts payment, and requests a rights object as is indicated by arrow 18. The requested rights object is downloaded to client A, arrow 19, and now the previously obtained content object can be used on client A. This concept of peer-to-peer distribution of content is called "super-distribution" and is considered a very important mechanism for the content based business.

Potentially, desirable and price-worthy content can spread rapidly in the population of users and create large revenue to the content providers/distributors.

Next the delivery mechanisms for download and streaming are described. These mechanisms are important to understand when considering the complications arising from managing rights

5 to media transported with respective mechanism.

In the case of download DRM in an IP network, the content object and the rights object are transported to the client using a reliable transport protocol such as the Hyper Text Transport Protocol (HTTP) or the File Transfer Protocol (FTP). These are standard web protocols used by most web servers and web browsers. HTTP and FTP both operate on top of the

10 Transmission Control Protocol (TCP), which handles all the data transfers. Optimized for non-real-time applications such as file transfer and remote log-in, TCP's goal is to maximize the data transfer rate while ensuring overall stability and high throughput of the entire network. To achieve this, using an algorithm called slow start, TCP first sends data at a low data rate, and then gradually increases the rate until the destination reports packet loss. TCP
15 then assumes it has hit the bandwidth limit or network congestion, and returns to sending data at a low data rate, then gradually increases repeating the process. TCP achieves reliable data transfer by re-transmitting lost packets. However, it cannot ensure that all resent packets will arrive at the client in a certain time e.g. to be able to be played in a media stream.

Now turning to the streaming technology. HTTP and FTP (or other protocols based on TCP)
20 is suited for reliable transfer of data but performs less well for streaming media, the main reasons being that TCP enforces reliable transport without regard to any timing requirements and that TCP changes the data transfer rate of the client server connection according to the availability of the bandwidth, not according to the need of the media. The most common standardized example for transport of real-time data is the Real-time Transport Protocol
25 [RTP], which is a packet format for multimedia data streams in an IP network. Most proprietary protocols for transporting real-time data are similar to RTP. In particular, RTP is a protocol framework to accommodate for additional functions. To completely specify the protocol requires additional information such as payload format (e.g. media encodings). Such information constitutes a so called "profile" for RTP. In streaming applications RTP
30 preferably runs on top of the User Datagram Protocol (UDP) which improves the streaming

experience compared to TCP. Unlike TCP, UDP is a fast, lightweight protocol without any re-transmission or data rate management functionality which makes it ideal for transmitting e.g. real-time audio and video data, which can tolerate lost packets. Because of the above mentioned slow start mechanism implicit in the TCP protocol, UDP traffic effectively gets
5 higher share of the bandwidth than the TCP traffic in a network.

For the sake of completeness the concept of "progressive download" should be mentioned. Progressive download means that the media is reliably downloaded, usually using TCP, but rendering is started before the downloading is complete. Since TCP is used also in this case, the same limitations apply for real-time media streams as was mentioned for download above.

10 To control the presentation of a transported multimedia stream, a control protocol is used such as the Real-Time Streaming Protocol [RTSP]. RTSP may be used for setting up a media streaming session, furthermore starting, pausing, stopping and moving ("fast forward" and "rewind") in the media stream. It can thus be thought of as a remote control between a client and a server or servers from which multimedia is being streamed.

15 In order to synchronize the streaming server and the client, the media client (which is a software part of the client) is required to have initialization parameters in order to correctly interpret the RTP data. These initialization parameters may be described with the Session Description Protocol [SDP], which is a description protocol for multimedia sessions, including among other things: session name, time during which the session is active, media
20 comprising the session, information to receive those media (addresses, ports, formats etc.), bandwidth used, type of media, codecs (algorithms for compression and decompression), - media keys and also additional attributes pertaining to a specific media in a multimedia stream or to an entire session.

Below is an example of an SDP description.

25 v=0
o=mobilemusic 288973739593 2887475859 IN IP4 126.16.64.4
s=Thesong
e=mobilemusic@themusiccompany.com
m=audio 0 RTP/AVP 0

a=control:rtsp://224.2.17.12/media/thesong.amr

The parameters have the following meaning:

'v' - version of the protocol

'o' - owner/creator and an identifier

5 's' - session name

'e' - e-mail address.

The 'm=' field is used to enumerate streams and contains information on payload type, RTP profile and recommended ports. RTP/AVP indicates that payload is RTP over UDP. The 'a=' field indicates attributes, 'a=control:' specifies the URL to the multimedia stream, in this case
10 an audio stream. Based on the information in this SDP description, the media client sends an RTSP SETUP command in order to establish the transport settings (IP address, port number, , and other parameters) and, after acknowledgement, an RTSP PLAY command to initiate the media stream is sent by the streaming server. Further details can be found in [RTSP] and [SDP].

15 A special case of the previous example is to just use the RTSP link URL:

rtsp://224.2.17.12/media/thehit.amr

to initiate the media stream.

Such a URL uniquely defines a streaming media and by using this data in a RTSP DESCRIBE message, a streaming session is initiated that will result in the same stream as in
20 the previous example. However, transport and protocol information must be negotiated between server and client before the RTSP SETUP and PLAY commands can be issued by the client. It will thus result in an additional round trip of messages between the client and server before the rendering can start (the DESCRIBE message and the reply). As a result, initiating a streaming session with only an RTSP URL, will cause an extra delay is therefore
25 not as efficient as the first case.

Another alternative to describe a streaming session is to use the Synchronization Multimedia Integration Language (SMIL) which is a media description language to describe a multimedia session. SMIL can be thought of as the Hyper Text Markup Language (HTML) specifying content and geometry of a web page, but adding to this a time based structure for multimedia

presentations, and thus enabling different streams to be specified and also different times to setting up the various streams (or render other media objects). Using SMIL also requires additional round trips of messages and is therefore less efficient. However, SMIL enables other types of multimedia sessions to be rendered than can be described by a single SDP description, for example time discrete objects like images.

Turning now to the protection of streaming media, encryption of data is usually required to maintain confidentiality of the media through a network. Encrypted data could in principle be transported with any protocol, but when the protocol is unreliable a loss of a packet may result in an impossibility to decrypt the data or a serious loss of quality, possibly much greater loss of quality than a corresponding loss of packet of unencrypted data. Depending on the encryption algorithm a lost packet may result in an error during decryption; which error may spread to other received packets making it impossible to decrypt these. This is in contrast to delivery of encrypted data when using a reliable protocol, where the entire data is guaranteed to be delivered. Therefore, special streaming encryption protocols are designed for wireless networks, an example being the Secure Real-Time Transport Protocol [SRTP], which is a profile of RTP. SRTP provides confidentiality, message authentication, and replay protection to RTP/RTCP traffic. It is designed to avoid error propagation due to errors in encrypted data, to be tolerant to loss or re-ordering of RTP packets and it allows fast-forward and rewind in an encrypted stream. SRTP transported over UDP is thus a secure, but unreliable, protocol.

An example of an SDP description to an SRTP encrypted streaming audio/video session:

```
i=The lord of the rings behind the scene
e=mobile_films@themusiccompany.com
a=recvonly
m=audio 0 RTP/SAVP 0
a=control:rtsp://224.2.17.12/media/lothringen.amr
k=base64:iO64Ygf+IJtfI8wSGbDaR==
m=video 0 RTP/SAVP 0
a=control:rtsp://224.2.17.12/media/lothringen.rtp
k=base64:Ah2pBY/HoqS+0g1bdG6TMg==
```

The major difference from the previous example is the SRTP profile, which is indicated by

RTP/SAVP in the "m=" fields. Also the individual encryption keys for the audio and the video streams are included in base 64 encoding in the "k=" fields.

Problem

The above described download technology is not immediately feasible for use with streaming technology. The separation of content and ticket is applicable to streaming.

The problem to be solved is thus: How to modify the download technology and its secure rights management to allow for (a) transmission of streaming multimedia and (b) secure rights management of the transmitted streamed multimedia taking the following facts in consideration:

- 10 - Streaming is a procedure that implies real time rendering of the media as it is received, streaming doesn't allow storage of the received media followed by rendering the media as with download.
- Existing network elements and mechanisms in use for download should, to the greatest extent possible, be reused also for streaming, thus allowing them to be used
- 15 simultaneously for download and streaming.
- Streaming media uses an unreliable transport protocol, such as user datagram protocol (UDP). A small amount of bit-errors or lost packets can be handled without major impact on the media quality and may be acceptable to the user if this can be controlled or at least verifiable so the user does not have to pay for too noisy media.
- 20 - However, as described the previously, in DRM systems some data cannot be transported unreliably, e.g. the usage rules and cryptographic media keys, to which no changes are acceptable, since that could violate the prescribed rules or make it impossible to decrypt the content.
- To cryptographically protect the streaming media a cryptographic key must be securely
- 25 agreed between the streaming server and client.
- If a secure streaming transport protocol is being used, the cryptographic key must be available before the streaming starts, but download DRM protocols are usually ignorant to the order of arrival of rights object and content object.
- It is desirable to be able to "rewind" and "fast-forward" the streaming media.

- In some applications, e.g. real-time applications, it is not possible to access the entire content at the same time (e.g. a web-cast). This should not affect the handling of the media.

In prior art DRM systems there are no common solutions to both DRM for download media and DRM for streaming media. Indeed, cryptographic protection of streaming media transported over channels with disturbances even without managing rights is hardly addressed (one exception being [SRTP]). In particular, given an existing system that provides DRM for download of content, there exists no solution to transparently incorporate DRM for streaming into this system. There are also other important constraints that should work transparently for both download and streaming, including mechanisms for super-distribution, preview of content and purchase of rights.

The present invention presents a solution to the above mention problem.

SUMMARY OF INVENTION

One object of the present invention is to provide a solution to handle DRM with streaming media.

Another object of the present invention to provide handling of DRM with streaming media by using existing protocols and protection mechanisms for DRM of media download.

Still another object of the invention is to provide handling of DRM with streaming media that allows for super-distribution of the streaming media.

Yet another object of the invention to provide an arrangement and a method for managing rights to streaming media.

A further object of the invention is to provide a system and a method of delivering and managing rights to streaming media.

These and other objects are achieved with the invention defined in the accompanying claims.

A distinguishing feature of the present invention is to use the DRM mechanism that comprises a content object and an associated rights object, wherein the content object comprises, not the content, but an initiation description of a forthcoming streaming session during which the digital media is transferred to a client by streaming. This feature will allow for preview and super-

distribution. Optionally the session initiation description comprises a cryptographic key for protection of the streaming media from unauthorized usage.

In the following the expression of "content" will occasionally denote whatever data located in the place where content is located in the content object in the prior art download DRM solution.

5 In the following the present invention is presented. To simplify the understanding, an existing given rights management system for download is assumed, using content objects and rights objects as described in the state of the art DRM solution for download. Rights to streaming media are managed by the following arrangement:

- 10 - Instead of the actual digital content in the content object, an initiation description of a streaming media is placed in the same location in the record. The initiation description may e.g. contain an SDP description, in particular a RTSP URL pointing to a particular streaming media, a SMIL file etc.
- The initiation description may optionally contain cryptographic information pertaining to protection of the streaming media from unauthorized usage.

15 Apart from this, the DRM solution for download is reused without changes. Thus e.g. the rights object contains usage rules and a cryptographic key encrypting the "content". Just as in the download case, the DRM agent parses the usage rules, decrypts the "content" and passes the clear text "content" on to the appropriate trusted application that will do the rendering. In the case of streaming media, the "content" is a streaming media initiation description.

20 Depending on trust model between the actors in a particular content distribution scenario, it may be sufficient with protecting the streaming initiation description as enabled by the download - DRM system, and no protection of the actual streaming media. Below are some examples of conditions that may, if complied with, either one or jointly, be considered substantial enough to neglect protection of the actual streaming media.

- 25 - If the streaming initiation description does not leak to unauthorized parties so as to only allow streaming to authorized parties.
- If it is sufficiently difficult to eavesdrop on the streaming media to deter or limit unauthorized usage.
- If it is sufficiently difficult to store the streaming media to deter or limit unauthorized
- 30 usage.

However, in the general case, in particular if only some or none of the conditions above a complied with, protection of a streaming media initiation description will not be sufficient and additional protection of the streaming media is necessary. Cryptographic protection of the streaming media can be applied at any level in the Open Systems Interconnect (OSI) model. In the following one example of this will be described, where protection is applied on the transport level.

A definite improvement of the security of streaming media is to cryptographically protect the media during transport between a streaming server managed by the content provider/distributor and trusted streaming application in the client. This may be achieved using a secure and (in particular for wireless networks) robust streaming transport protocol such as SRTP, as previously described. In this case it is of course vital that the cryptographic key or keys used to protect the streaming media between streaming server and client are kept confidential with the trusted parties. This can be (or be managed by) the cryptographic information that the invention optionally specifies to be included in the streaming media initiation description. E.g. an SDP description has optional attributes for specification of media keys, as indicated in one of the previous examples. In particular such an initiation description contains only one or several RTSP URL(s) and an encryption key attribute(s) containing encryption key(s). Alternatively cryptographic keys can be conveyed in a streaming media initiation description together with any initiation description of a clear text streaming session, e.g. an SDP description without key attributes bundled with a cryptographic key, in particular one or several RTSP URL(s) and separate encryption key(s). An alternative embodiment of streaming media initiation description is a SMIL file bundled with cryptographic key(s).

Additional security mechanisms can also be considered to protect the streaming media initiation description or streaming media itself.

Advantages achieved with the invention

The present invention is generally applicable to rights management (DRM) of streaming media. The invention provides a common solution for DRM for media download and DRM for streaming media. With the present invention, very few changes are needed in an existing DRM for download system to enable a compatible system that handles streaming media.

Because of this and the particular way that these changes seamlessly fit into the concepts of

DRM for download, all features of the DRM download systems such as rights management, super-distribution, preview, purchase of rights objects to a particular content etc. carry over to streaming media. E.g. super-distribution generally works by forwarding of content object from peer to peer. The receiving peer can with a purchased rights object initiate a streaming session of his/her own.

A word of explanation may be necessary for the concept of preview of streaming. This may be implemented in several ways. One way is to actually provide the content object with a limited multimedia sample of the full content or related content that is actually downloaded to the client. Another way is to provide a key with which the client can setup a temporally or otherwise limited/restricted stream, optionally at a lower resolution/quality than the full version.

The invention also provides as an option to enable cryptographic protection of the media stream and solves the key management problem how to establish common secret keys at the streaming server and streaming client. Since the arrangement is compatible with the use of secure and robust streaming protocols such as SRTP, the invention is perfectly adequate for managing rights in wired networks as well as wireless networks with disturbances causing errors in transmissions.

As previously explained there are a number of differences between streaming and downloading of media content. However, the user experiences of the same media, say a video of a musical concert, being rendered by either method need not differ significantly: The concert downloaded to the client has the advantage of not showing any signs of occasional disturbances whereas a video that was streamed to the client can be a live and directly broadcasted concert.

In accordance with the invention, one and the same rights management scheme may be used for both download and streaming media independently of transport of media. This rights management scheme will work for super-distribution, purchasing of rights etc. which are considered important business cases. If super-distribution only would work for download, then the introduction of streaming services would potentially lead to an uncertainty of the capabilities to distribute/purchase content that could damage the business case for super-distribution of download content.

Since the same rights management scheme is used for both download and streaming media it is not necessary to implement parallel solutions for download and streaming. That could also vouch for a unified user experience.

BRIEF DESCRIPTION OF THE DRAWINGS

- 5 The invention together with further objects and advantages thereof, may best be understood by making reference to the following description taken together with the accompanying drawings, in which:

Fig. 1 illustrates the data structure of a rights management (DRM) system using prior art download technology,

- 10 Fig. 2 illustrates the nodes involved in prior art DRM,

Fig. 3 is a diagram illustrating the prior art method steps used for access to content from a content distributor, in a DRM system using the download technology

Fig. 4 is a diagram illustrating the prior art method steps used for access to content from another client (super-distribution), in a DRM system using the download technology,

- 15 Fig. 5 illustrates schematically the basic DRM mechanism for streaming media in accordance with the present invention,

Fig. 6 is a diagram illustrating the method steps in accordance with the present invention for transmission of streaming media and DRM,

- 20 Fig. 7 is a schematic block diagram illustrating nodes and devices for providing DRM of streaming media in accordance with the invention, and

Figs. 8A-D illustrate various methods of including an initiation description in a content object in accordance with the invention, and

Figs. 9A-F illustrate various methods of including an initiation description with a cryptographic media key in a content object in accordance with the invention.

- 25 Description of preferred embodiments

Fig. 5 illustrates the data structure and a client view of an example of DRM for streaming media in accordance with the present invention. For the moment it is assumed that the client has received a content object 20 and a rights object 2 to a particular digital multi-media which

is transported from a streaming server 21 to the client in data packets 22 during a streaming session. How this situation arises will be described further down.

The content object comprises meta-data, an initiation description 23 in the form of an SDP description of the kind described above including a media key 24. The initiation description is
5 cryptographically protected as symbolized by the heavy rectangle 25.

The rights object associated with the content object comprises meta-data, usage rights and a content key, just as in the download DRM case.

The client uses the content key provided in the rights object to decrypt the protected
initialisation description including the media key provided in the content object. The clear text
10 media key is used by the client for decryption of the protected multi-media stream 22. The
decrypted media stream is accessed by an application and is rendered on a non-shown media
player.

Before the multi-media stream is delivered to the client a streaming media session must be set
up. To this end a connection between the client and a streaming server is set up. Over this
15 connection many kinds of information relating to the multi-media, such as its name, its type,
where it is located, the manner in which it is coded etc., are exchanged between the streaming
server and the client before the media stream is started. The initiation description is used for
these purposes.

Fig. 6 illustrates method steps in accordance with the present invention for providing DRM
20 with streaming media. The client sends a request for a multimedia to a distribution server as
illustrated at arrow 26. The terms for the rights to the requested multimedia are negotiated and
settled upon. Next step, illustrated by arrow 27, is that the distribution server transmits the
content object with the protected initiation description to the client. Next the rights object
containing the usage rights and the content key is sent to the client, as represented by arrow
25 28. Using said content key the client decrypts the session initiation description and using the
information given therein the client initiates the set up of a streaming session with a streaming
server. This is indicated by the double headed arrow 29. Over this connection further
parameters to be used in the streaming session are exchanged. In the last step the streaming
session is started and a protected multi-media stream of packets starts streaming to the client,
30 illustrated by arrow 30.

The packets are transported on the streaming protocol indicated in initiation description, in this case the SRTP protocol. A reliable protocol is used for transport of the rights object and the content object, e.g. HTTP or WAP. A reliable protocol is also used for RTSP control signalling.

- 5 The client may verify receipt of the packets by sending an acknowledgement or verification to the streaming server. Such mechanisms are part of the SRTP/SRTCP protocol [SRTP].

Fig. 7 is block diagram illustrating nodes and devices for providing DRM of streaming media in accordance with the invention. There is a content server 31 containing multi-media, a streaming server 32 providing a multi-media stream, an encryption key generator 33

- 10 providing content keys as well as media keys, a media key database 34 for storing media keys, a content object generator 35, a rights object generator 36, a distribution server 37 and a rights server 38.

The content object generator fetches the above mentioned initialization parameters for use in the initiation description of a streaming session from the content server 31 (illustrated by

15 arrow 39). The media key 24 is fetched from the key generator. The initiation description is cryptographically protected using a content key also generated by the key generator. This content key is also available for rights object generator, see below. Meta-data are also fetched and are included in the content object. The generated content object is stored in the distribution server and a copy thereof is delivered to the client in accordance with arrow 27 of

- 20 Fig. 6.

The rights object generator generates the rights object associated with the content object and includes therein the same content key as used for the protection of the content object. The rights object, which includes an identity, is stored in the distribution server and in the rights server. A copy thereof is delivered to the client in accordance with arrow 28 of Fig. 6.

- 25 Double headed arrow 40 illustrates delivery of the media and content keys to the content object generator and the rights object generator.

The media key inserted into the content object is also stored in the media key database together with the identity of the rights object associated with the generated content object. This is illustrated with arrow 41 in Fig. 7.

Up to now the situation is the following: The client has received the content object and the rights object as previously described (arrows 27 and 28 of Fig. 6). The media key 24 and related rights object identity are stored in the media key database.

- Next, at arrow 29 in Fig. 7 (which corresponds to arrow 29 in Fig. 6), a session set up message from the client is received by the streaming server. This message contains the previously mentioned information and subsequent signalling between client and server will reveal the identity of the rights object associated with the content object. The streaming server sends a media key request, arrow 42, to the media key database and provides the rights object identity received at arrow 29. In response to this request the media key database is searched for the indicated rights object identity and returns the corresponding media key to the streaming server, as indicated by arrow 43. The streaming server will now use this media key to cryptographically protect the media stream it starts to deliver to the client, arrow 30 (corresponding to arrow 30 in Fig. 6). The streaming server and the client will now both use the same media key for encryption and decryption respectively.
- Many modifications of the above described example are possible. Instead of using the same media key for encryption at the streaming server and for decryption at the client the streaming server may use a public media key while a private media key is delivered to the client in the content object.

- Another modification is to cryptographically protect also the media key in the content object instead of providing it in clear text as described.

The media stream and/or the content object may also be protected by encryption and/or integrity protection. The rights object and/or the content object may also be delivered to the client unprotected.

- The order in which the content and rights objects are delivered to the client may be reversed, i.e. step 28 may precede step 27 in Fig. 6. They may also be delivered to the client over separate communication channels, such as in a SMS message and using the WAP protocol respectively, in a mobile communication network.

The initiation description may be provided by the content server instead of being provided by the content object generator.

In Fig. 8 different embodiments of the content object are shown at 8A-8D. A common feature for all embodiments in Fig. 8 is that no cryptographic information is contained in the initiation description. At Fig. 8A a basic version is shown which contains the usual meta-data and the initiation description file, this time without media key. In Fig 8B the initiation description is embodied as an SDP description with no key attributes set. In Fig. 8C the initiation description is embodied as a SMIL file without key. Fig. 8D is a special case of Fig. 8B wherein the SDP description is a RTSP URL that addresses the streaming media.

In Fig. 9 further different embodiments of the content object are shown at 9A-9F. A common feature for all embodiments is that cryptographic information is contained in the initiation description. At Fig. 9A a basic version is shown which contains the usual meta-data and the initiation description file including a media key. In Fig. 9B the initiation description is embodied as an SDP description containing key attributes that are set. In Fig. 9C the initiation description is embodied as an SDP description with no key attributes set; the media key is included separately in the initiation description. In Fig. 9D the initiation description is provided as a SMIL file and a media key. Fig. 9E is a special case of Fig. 9B wherein the SDP description is an RTSP URL that addresses the streaming media and that has media key attributes set. Similarly Fig. 9F is a special case of Fig. 9C wherein the SDP description is an RTSP URL addressing the streaming media. The media key is provided separately from the RTSP URL in the initiation description.

It should be understood that the media key shown in Fig. 9 may comprise several further keys such as for examples further media keys and/or further keys for providing other types of security. One reason for using several media keys is to associate each key with a just a portion of the complete media stream so as to enhance the security. The idea behind this is that it should not be possible for an eavesdropper to decrypt the entire media stream using a single key.

The embodiments described above are merely given as examples, and it should be understood that the present invention is not limited thereto. Further modifications, changes and improvements, which retain the basic underlying principles disclosed and claimed herein are within the scope and spirit of the invention.

References

[HAC] A.J. Menezes, P.C. van Oorschot and S.C. Vanstone, "Handbook of Applied Cryptography", CRC Press.

- [RTP] V. Jacobson, S.L. Casner, R. Frederick and H. Schulzrinne, "RTP: A Transport Protocol for Real-Time Applications", RFC 1889, IETF, November 2001.
- [RTSP] H. Schulzrinne, A. Rao, R. Lanphier, "Real Time Streaming Protocol (RTSP)", RFC 2326, IETF, April 1998.
- 5 [SDP] M. Handley, V. Jacobsson, "SDP: Session Description Protocol", RFC 2327, IETF, April 1998.
- [SRTP] M. Baugher, R. Blom, E. Carrara, D. McGrew, M. Näsland, K. Norrman and D. Oran "The Secure Real Time Transport Protocol", draft-ietf-avt-srtp-05.txt, IETF, June 2002.

CLAIMS

1. An arrangement for managing rights to streaming media using a management mechanism based on a content object and a rights object, where said content object comprises means for initiation of said streaming media and said rights object comprises usage rules defining the rights to use said content object and/or said streaming media.
5
2. An arrangement in accordance with claim 1 wherein said initiation means comprises a session description of the streaming media, an SDP description, a URL to said streaming media or a SMIL file.
3. An arrangement in accordance with claim 1 or 2 wherein said rights object contains first cryptographic data related to cryptographic protection of at least a portion of said content object.
10
4. An arrangement in accordance with claim 3 wherein said content object further comprises second cryptographic data for cryptographic protection of said streaming media.
5. An arrangement in accordance with claim 4, wherein said second cryptographic data comprises at least one cryptographic key.
15
6. An arrangement in accordance with claim 4, wherein said second cryptographic data comprises several cryptographic keys protecting the streaming media.
7. A method of managing rights to streaming media using a management mechanism based on a rights object and an associated content object, said rights object comprising usage rules defining the rights to use said content object and/or said streaming media, said method further comprising the step of providing said content object with an initiation description for said streaming media.
20
8. A method in accordance with claim 7 wherein said initiation description is provided in the form of a session description of the streaming media, an SDP description, a URL to said streaming media or a SMIL file
25
9. A method in accordance with claim 7 or 8 comprising the further steps of cryptographically protecting at least a portion of said content object and providing said rights object with first cryptographic data used for said protection.

10. A method in accordance with claim 9 comprising the further step of cryptographically protecting said first cryptographic data.
11. A method in accordance with claim 9 comprising the further steps of cryptographically protecting said streaming media and providing said content object with second cryptographic data used for said streaming media protection.
12. A method in accordance with claim 11 comprising the step of further protecting said streaming media using a security protocol.
13. A method in accordance with claim 12 wherein said security protocol is the secure real time transport protocol (SRTP).
14. The method in accordance with claim 7 comprising the further step of transmitting the content object as a downloadable object in a rights management system for download, thereby reusing the mechanisms for rights management of said latter system for rights management in a system for transmission of streaming media.
15. The method in accordance with claim 7, comprising the further steps of providing said content object with a portion of said digital media, and transmitting said content object so provisioned to a user who has no rights or limited rights to said digital media.
16. The method in accordance with claim 7, wherein the content object and/or rights object is protected by encryption and/or integrity protection.
17. A system for delivering digital streaming media and for managing rights to said digital media, wherein management of the rights uses a mechanism based on rights object and an associated content object, comprising:
- server means for providing said streaming media,
 - means for generating a content object
 - means for generating a rights object,
 - means for generating content key means for use in cryptographic protection of at least part of said content object and for generating media key means for use in cryptographic protection of said media when streamed,
- said system further comprising:
- means for generating an initiation description for said streaming media, and

- means for storing said media key means and for allowing retrieval of said stored media key means for use in said cryptographic protection of said streaming media.

18. A system in accordance with claim 17, wherein said initiation description means generates a session description of the streaming media, an SDP description, a URL to said streaming
5 media or a SMIL file.

19. A method of delivering and protecting digital media using a management mechanism based on content object and a rights object, said digital media being streamed from a streaming server to a client, the method also allowing rights management of the streamed digital media and/or management of said content object, said method comprising the steps of:

10 -the client requesting delivery of the digital media at a distribution server that contains information on the digital media,

- said distribution server in response to said request delivering to the client a content object comprising a first portion containing meta data and a second portion containing a initiation description for the streaming media and cryptographic media key means for use in protection
15 of the streaming media, said content object being protected with cryptographic content key means,

- said distribution server in response to said request also delivering to the client a rights object containing usage rules defining the rights to use said content object and/or said streaming media, said rights object further comprising said content key means,

20 - the client upon receipt of the rights object and the content object enforcing the rights to the content object and/or streaming media based on the information contained in said rights object and accessing said content object by using said content key means so as to read said initiation description,

- the client, in response to reading of said description, initiating streaming media by setting up
25 a connection between the client and said streaming server,

- said streaming server, following the set up of said connection, protecting the streaming media using said media key means and delivering the so protected streaming media to the client,

- the client upon receipt of the protected streaming media accessing the digital media using
30 said media key means and rendering the accessed streaming media according to said usage rules.

20. The method in accordance with claim 19 comprising the further step of including in said initiation description:

- a URL of the streaming media; and/or
- metadata pertaining to the set up of a connection between said server and the client; and/or
- 5 - a reference to a streaming media protocol for transport of the streaming media from the said server to the client; and/or
- codec information on the streaming media.

21. The method in accordance with claim 19 comprising the further step of protecting said streaming media using a security protocol.

- 10 22. The method in accordance with claim 19, wherein said initiation description is provided in the form of an SDP description (Session Description Protocol) describing the streaming session of said streaming media.

23. The method in accordance with claim 22, wherein said cryptographic media key means is contained in the SDP description.

- 15 24. The method in accordance with claim 22, wherein said cryptographic media key means is provided separately from the SDP description.

25. The method in accordance with claim 19, wherein said initiation description is provided in the form of a SMIL file.

- 20 26. The method in accordance with claim 25, wherein said cryptographic media key means is contained in said SMIL file.

27. The method in accordance with claim 25, wherein said cryptographic media key means is provided separately from said SMIL file.

28. The method in accordance with claim 19, wherein the initiation description is provided in the form of a URL to said streaming media.

- 25 29. The method in accordance with claim 19, wherein several cryptographic media keys means are used for protection of the streaming media.

30. The method in accordance with claim 19 comprising the further step of including in the initiation description information on management of said cryptographic media key means,

said information allowing for cryptographic protection of the streaming media and/or verification of data integrity of the streaming media with a new key derived from said first key.

5 31. The method in accordance with claim 19 comprising the further step of including in the meta data portion of the content object the URL (Uniform Resource Locator) of a distribution server.

32. The method in accordance with claim 19, wherein a user of said client transmits the content object to a second user.

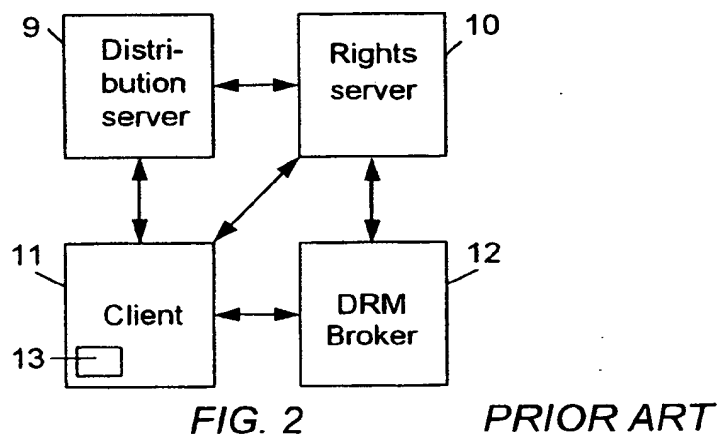
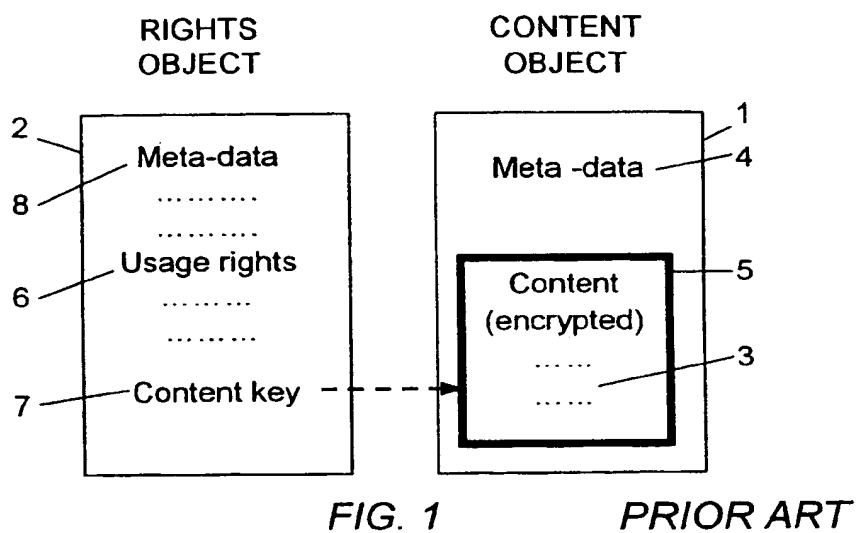
10 33. The method in accordance with claim 19 comprising the further step of using a secure real time transport protocol (SRTP) as streaming transport protocol.

34. The method in accordance with claim 19, wherein said cryptographic media key means is used to derive cryptographic information in order to integrity protect and/or verify reception of the streaming digital media.

15 35. The method in accordance with claim 19, wherein the content object and rights object are delivered to the client using HTTP (Hypertext Transfer Protocol) and/or WAP (Wireless Application Protocol) and/or SMS (Short Message Service).

36. The method in accordance with claim 19, wherein the content object and/or streaming digital media is protected by encryption and/or integrity protection.

20 37. The method in accordance with claim 19, wherein the rights object and/or content object is delivered to the client unprotected.



2/5

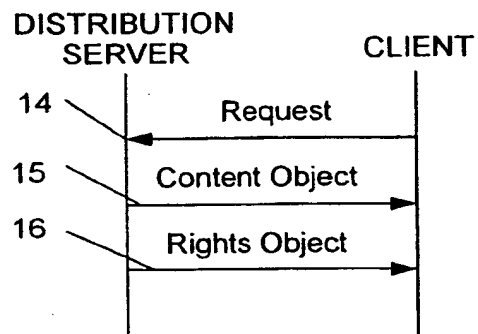


FIG. 3

PRIOR ART

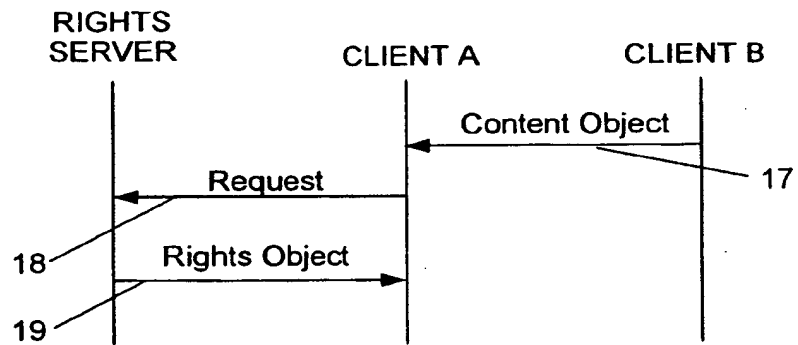


FIG. 4

PRIOR ART

3/5

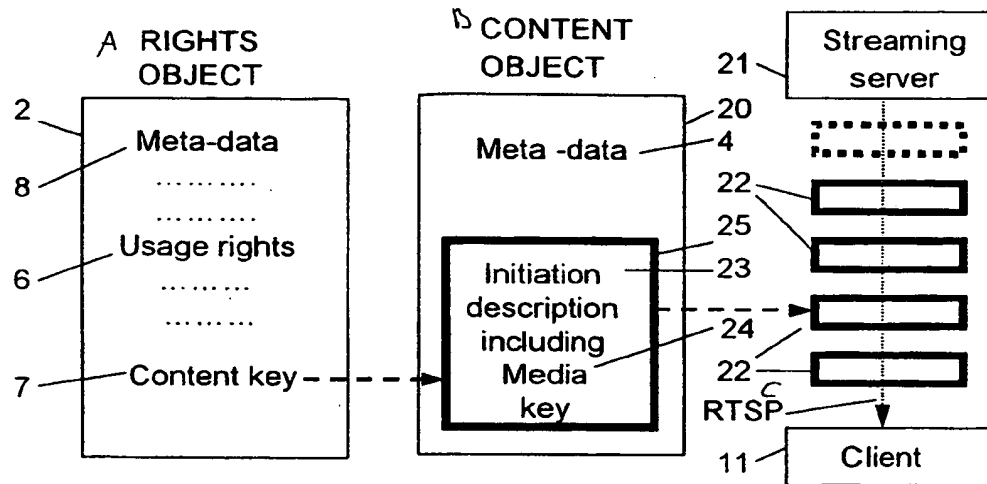


FIG. 5

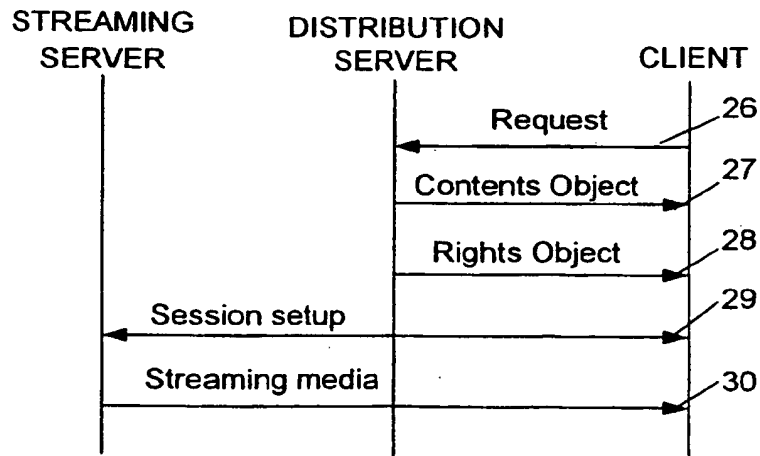


FIG. 6

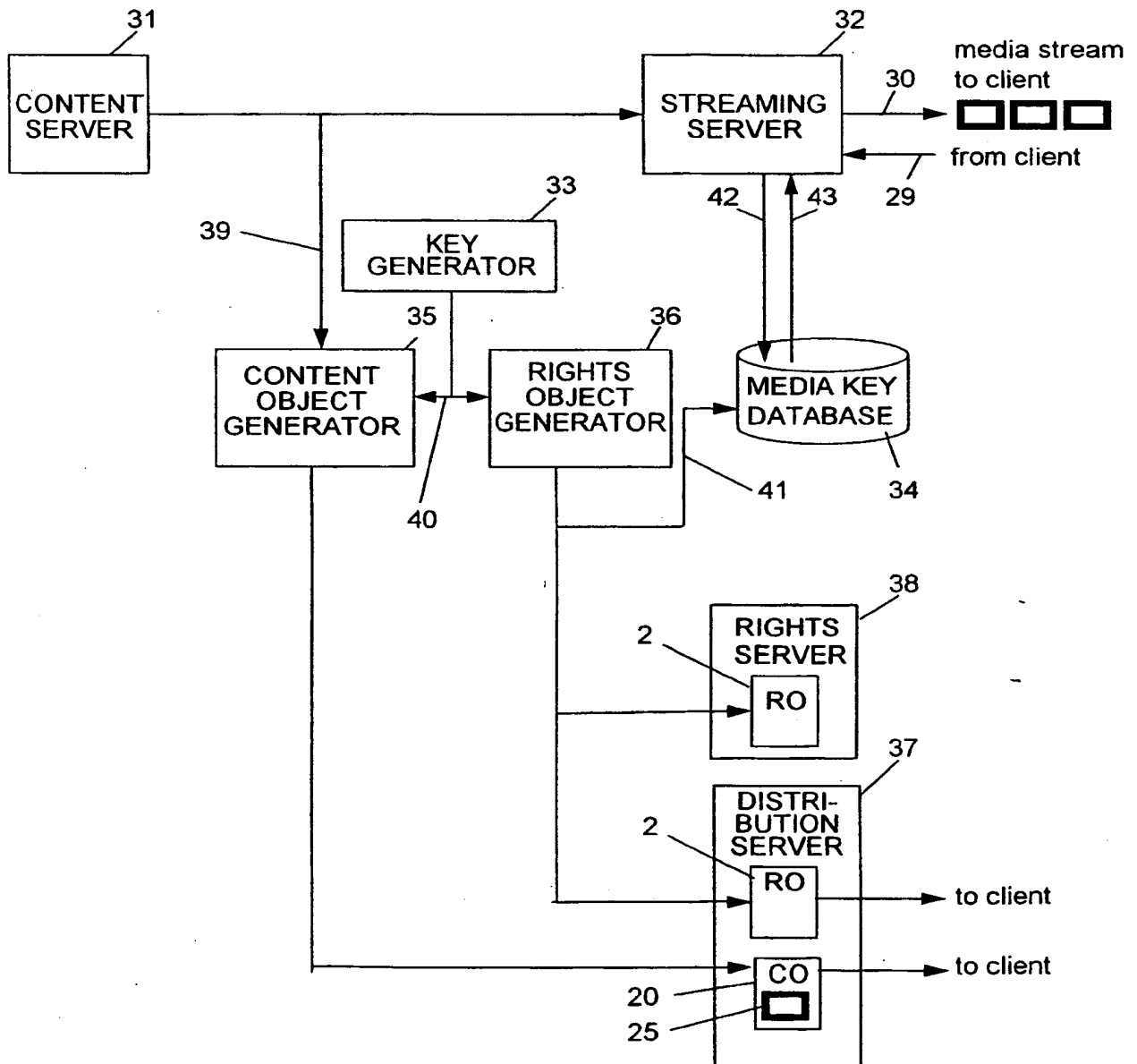


FIG. 7

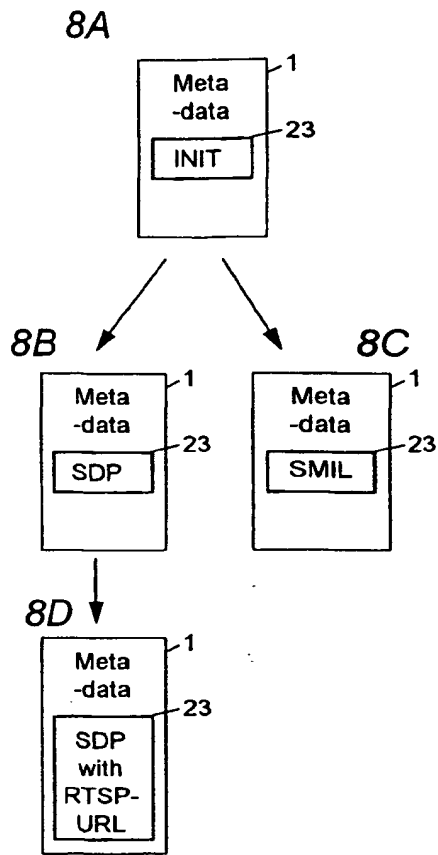


FIG. 8

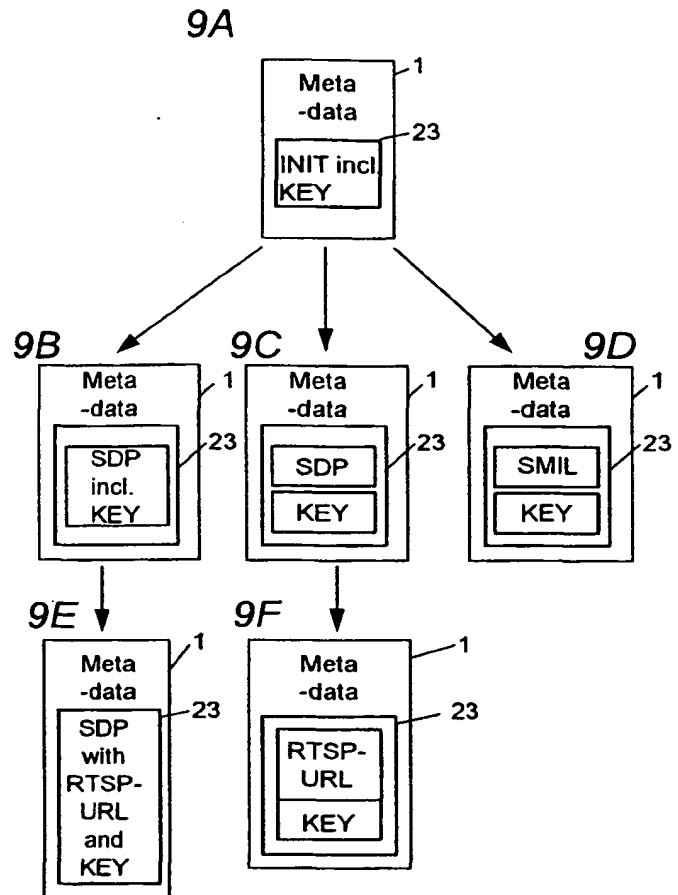


FIG. 9